

FILED

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

2019 DEC 18 A 8:42

CLERK OF DISTRICT COURT  
ALEXANDRIA, VIRGINIA

MICROSOFT CORPORATION, a  
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING  
A COMPUTER NETWORK  
THEREBY INJURING PLAINTIFF  
AND ITS CUSTOMERS,

Defendants.

Civil Action No:

1:19cv1582 LO/JFA

**FILED UNDER SEAL PURSUANT  
TO LOCAL CIVIL RULE 5**

**COMPLAINT**

Plaintiff MICROSOFT CORP. (“Microsoft”) hereby complains and alleges that JOHN DOES 1-2 (collectively “Defendants”), have established an Internet-based cyber-theft operation referred to as “Thallium.” Through Thallium, Defendants are engaged in breaking into the Microsoft accounts and computer networks of Microsoft’s customers and stealing highly sensitive information. To manage and direct Thallium, Defendants have established and operate a network of websites, domains, and computers on the Internet, which they use to target their victims, compromise their online accounts, infect their computing devices, compromise the security of their networks, and steal sensitive information from them. Internet domains used by Defendants to operate Thallium are set forth at **Appendix A** to this Complaint and are referred to as the “Command and Control Infrastructure.” Microsoft alleges as follows:

**NATURE OF THE ACTION**

1. This is an action based upon: (1) the Computer Fraud and Abuse Act, 18 U.S.C. §

1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) Cybersquatting under the Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d); (7) Common Law Trespass to Chattels; (8) Unjust Enrichment; (9) Conversion; and (10) Intentional Interference with Contractual Relationships. Plaintiff seeks injunctive and other equitable relief and damages against Defendants who operate and control a network of computers known as the Thallium Command and Control Infrastructure. Defendants, through their illegal activities involving Thallium, have caused and continue to cause irreparable injury to Microsoft and its customers, and the public.

#### **PARTIES**

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. On information and belief, John Doe 1 controls the Thallium Command and Control Infrastructure in furtherance of conduct designed to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 1 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

4. On information and belief, John Doe 2 controls the Thallium Command and Control Infrastructure in furtherance of conduct designed to cause harm to Microsoft, its customers, and the public. Microsoft is informed and believes and thereupon alleges that John Doe 2 can likely be contacted directly or through third-parties using the information set forth in **Appendix A**.

5. Third parties VeriSign, Inc., VeriSign Information Services, Inc., and VeriSign Global Registry Services (collectively, “VeriSign”) are the domain name registries that oversee the registration of all domain names ending in “.com” and “.net” and are located at 12061 Bluemont Way, Reston, Virginia 20190.

6. Third party Public Interest Registry is the domain name registry that oversees the registration of all domain names ending in “.org,” and is located at 1775 Wiehle Avenue, Suite 100, Reston, Virginia 20190.

7. Third party .Club Domains, LLC is the domain name registry that oversees the registration of all domain names ending in “.club,” and is located at 100 SE 3rd Ave. Suite 1310, Fort Lauderdale, Florida 33394.

8. Third party Afiliat Limited c/o Afiliat USA, Inc. is the domain name registry that oversees the registration of all domain names ending in “.info” and “.mobi,” and is located at 300 Welsh Road, Building 3, Suite 105, Horsham, Pennsylvania 19044.

9. Third parties Binky Moon, LLC and Donuts Inc. (collectively “Donuts”) are the domain name registries that oversee the registration of all domain names ending in “.cash,” and are located at 5808 Lake Washington Blvd NE, Suite 300, Kirkland, Washington 98033.

10. Third party Neustar, Inc. is the domain name registry backend that oversees the registration of all domains ending in “.biz.” Neustar, Inc. is located at 21575 Ridgetop Circle, Sterling, Virginia 20166.

11. Set forth in **Appendix A** are the identities of and contact information for third party domain registries that control the domains used by Defendants.

12. On information and belief, John Does 1-2 jointly own, rent, lease, or otherwise have dominion over the Thallium Command and Control Infrastructure and related infrastructure and through those control and operate Thallium. Microsoft will amend this complaint to allege

the Doe Defendants' true names and capacities when ascertained. Microsoft will exercise due diligence to determine Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

13. Microsoft is informed and believes and thereupon alleges that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that Microsoft's injuries as herein alleged were proximately caused by such Defendants.

14. On information and belief, the actions and omissions alleged herein to have been undertaken by John Does 1-2 were actions that Defendants, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, provided assistance and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

#### **JURISDICTION AND VENUE**

15. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of The Computer Fraud and Abuse Act (18 U.S.C. § 1030), Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the Anticybersquatting Consumer Protection Act (15 U.S.C. § 1125(d)). The Court also has subject matter jurisdiction over Microsoft's claims for trespass to chattels, conversion, unjust enrichment, and intentional interference with contractual

relationships pursuant to 28 U.S.C. § 1367.

16. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Microsoft's claims has occurred in this judicial district, because a substantial part of the property that is the subject of Microsoft's claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Defendants maintain Internet domains registered in Virginia, engage in other conduct availing themselves of the privilege of conducting business in Virginia, and utilize instrumentalities located in Virginia and the Eastern District of Virginia to carry out acts alleged herein.

17. Defendants have affirmatively directed actions at Virginia and the Eastern District of Virginia by directing their activities, including theft of information, at individual users located in the Eastern District of Virginia and directing malicious computer code at the computers of individual users located in Virginia and the Eastern District of Virginia and attempting to and in fact infecting those user computers with the malicious computer code and instructions to Microsoft's Windows operating system, the computing devices and high-value computer networks of individual users and entities located in Virginia and the Eastern District of Virginia, in order to compromise the security of those systems and to steal sensitive information from those networks, all to the grievous harm and injury of Microsoft, its customers and licensees, and the public.

18. Defendants maintain certain of the Thallium Command and Control Infrastructure registered through VeriSign, Public Interest Registry and Neustar which reside in the Eastern District of Virginia. Defendants use these domains to communicate with and control the Thallium-infected computers that Defendants communicate with, control, steal from, update, and maintain in this judicial district. Defendants have undertaken the acts alleged herein with

knowledge that such acts would cause harm through domains located in the Eastern District of Virginia, through the Thallium domains maintained through facilities in the Eastern District of Virginia, and through user computers located in the Eastern District of Virginia, thereby injuring Microsoft, its customers and member organizations, and others in the Eastern District of Virginia and elsewhere in the United States. Therefore, this Court has personal jurisdiction over Defendants.

19. Pursuant to 28 U.S.C. § 1391(b), venue is proper in this judicial district. A substantial part of the events or omissions giving rise to Microsoft's claims, together with a substantial part of the property that is the subject of Microsoft's claims, are situated in this judicial district. Venue is proper in this judicial district under 28 U.S.C. § 1391(c) because Defendants are subject to personal jurisdiction in this judicial district.

## **FACTUAL BACKGROUND**

### **Microsoft's Services And Reputation**

20. Microsoft® is a provider of the Windows® operating system, the Hotmail®, Outlook®, and MSN® email and messaging services and the Office 365® and Azure® cloud-based business and productivity suite of services, as well as a variety of other hardware products, software and services, including under the Surface®, Xbox®, and HoloLens® brands and trademarks. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand,

including Microsoft,<sup>®</sup> Windows,<sup>®</sup> Hotmail<sup>®</sup>, Outlook,<sup>®</sup> MSN,<sup>®</sup> Office 365,<sup>®</sup> Azure,<sup>®</sup> Surface,<sup>®</sup> Xbox,<sup>®</sup> and HoloLens.<sup>®</sup> Copies of the trademark registrations for these trademarks are attached as **Appendix B** to this Complaint.

### **Thallium**

21. Thallium specializes in targeting, penetration, and stealing sensitive information from high-value computer networks connected to the Internet. The precise identities and locations of those behind the activity are generally unknown but have been linked by many in the security community to North Korean hacking group or groups. Thallium targets Microsoft customers in both the private and public sectors, including businesses in a variety of different industries. Thallium has targeted government employees, organizations and individuals that work on Nuclear Proliferation issues, think tanks, university staff members, members of organizations that attempt to maintain world peace, human rights organizations, as well as many other organizations and individuals. Thallium has been active since 2010, and it poses a threat today and into the future.

22. Thallium operates in the following fashion: after researching a victim organization, Thallium will identify individuals employed by that organization through publicly available information and by social-media interaction. Microsoft has observed fake email addresses being created to connect with possible victims and other potential targets. Thallium typically attempts to compromise the accounts of targeted individuals through a technique known as “spearphishing.” In a typical spearphishing attack, Thallium sends the targeted individual an email specifically crafted to appear as if it was sent from a reputable email provider (ex. Hotmail, Gmail, Yahoo). The threat actors frequently send emails that state that there is a problem with the victim’s account and/or suspicious login activity was detected. By gathering information about the targeted individuals from social media, public personnel directories from organizations

the individual is involved with, and other public sources, Thallium is able to package the spearphishing email in a way that gives the email credibility to the target. In many other cases, Thallium has created emails that appear to have been sent from a familiar contact known by the targeted user.

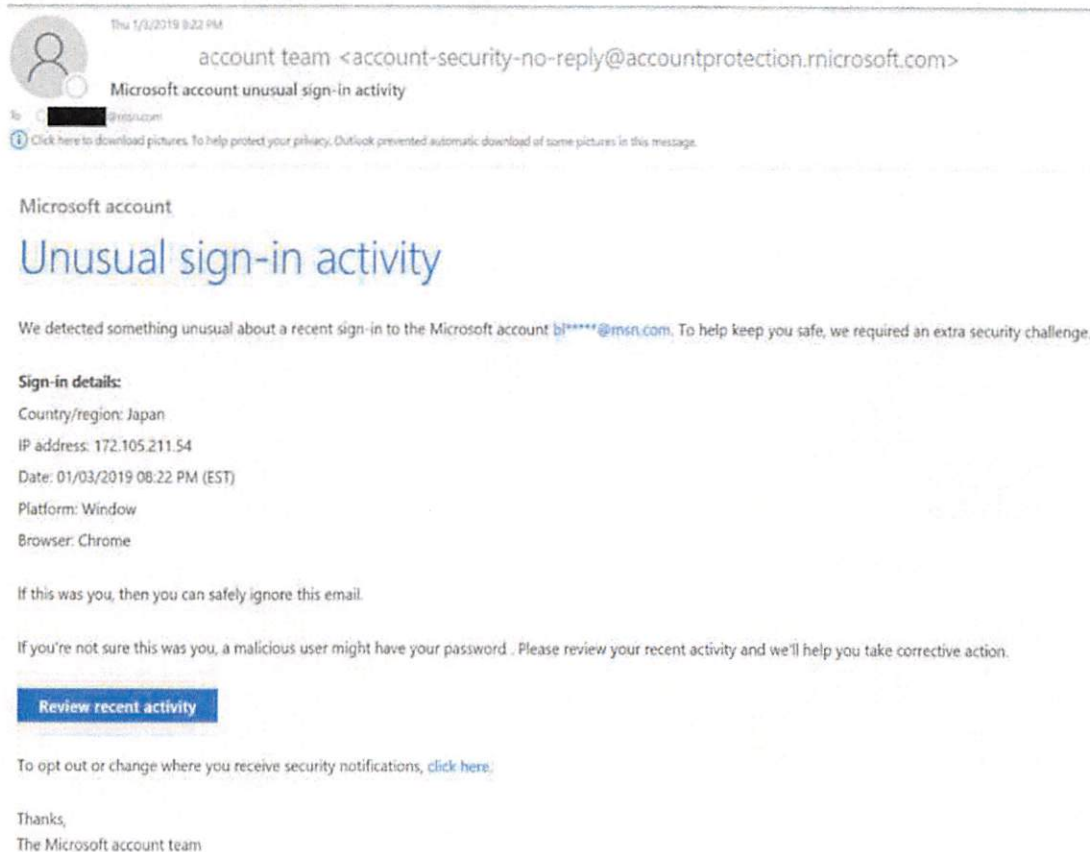
23. Thallium sends these emails from a variety of online email services which also include Hotmail, Gmail and Yahoo. The spearphishing emails often include links to websites that Thallium has set up in advance and that it controls. When a victim clicks on the link in the email, their computer connects to the Thallium-controlled website. The victim is then presented with a copy of a login page for the webmail provider that the victim is a subscriber of (e.g. Hotmail, Yahoo, Gmail, United Nations webmail<sup>1</sup>).

24. **Figure 1** below shows a copy of a spearphishing email used by Thallium. The email was sent on January 3, 2019 and is spoofed to appear as if it was sent from a Microsoft Account Team. For example, in the email address from which the email was sent, the Thallium defendants have combined the letters “r” and “n” to appear as the first letter “m” in “microsoft.com.” Side by side, the letters “r” and “n” (*i.e.* “rn”) appear very similar to the letter “m.”

---

<sup>1</sup> Thallium is targeting individuals with email addresses associated with the United Nations and their @un.org domains.





### Figure 1 – Sample Spearphishing Email

25. By clicking on the links seen in the above examples, the targeted user will be connected to a Thallium-controlled website which will attempt to induce the victim to enter their account credentials. For example, in **Figure 1** above, the targeted user would have been taken to the following domain that is a masquerade of Hotmail.com: *login.hotrnall.com*

26. Upon successful compromise of a victim account, Thallium frequently logs into the account from one of their IP addresses to review emails, contact lists, calendar appointments, and anything else of interest that can be found in the account. On multiple occasions, Thallium has also created a new mailbox rule in the victim's account settings. This mailbox rule will forward all new emails received by the victim to Thallium-controlled email addresses which are included in the auto-forward rule. In this way, Thallium immediately receives copies of emails

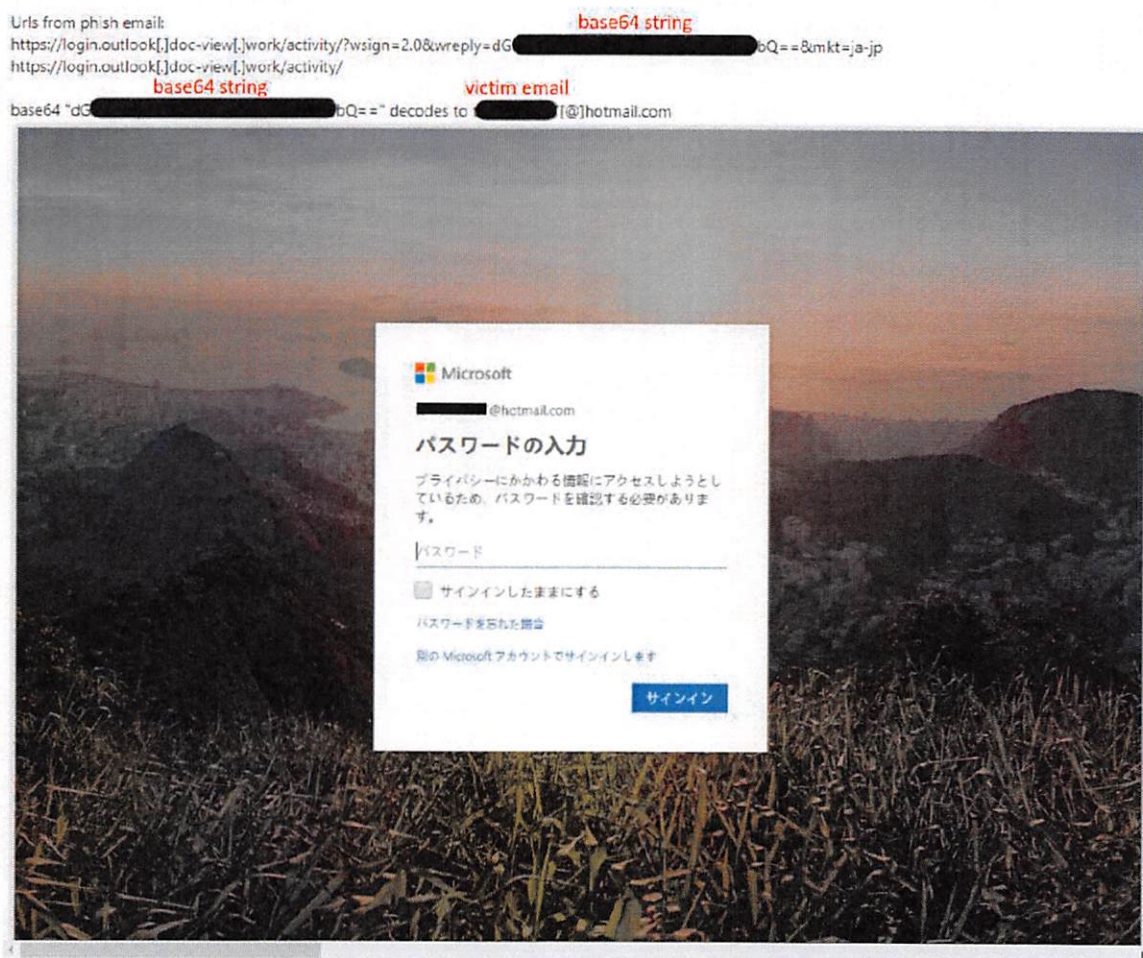
received by the victim, and Thallium can store and review that stolen material on Thallium-controlled computers, beyond the control of the victim.

27. Thallium often keeps track of which links have been sent to which victims by including a Base64 hash<sup>2</sup> of the victim email address in the URL path of the link in the spearphishing email. This allows Thallium to verify quickly which victims have received and opened the spearphishing email and clicked on the link within. **Figure 2** below shows an example of a link with the victim email address Base64 hash included in the URL path.<sup>3</sup>

---

<sup>2</sup> A “hash” is a mathematical function that can be used to map data of arbitrary size to fixed-length values. “Base64” is an encoding scheme by which, for example, text such as an email address can be represented through corresponding Base64 alphanumeric character values.

<sup>3</sup> In Figure 2, the first and last characters of the Base64 hash are shown for illustrative purposes, but the complete Base64 hash is obfuscated to preserve the privacy of the victim and plaintiff’s operational security, as the Base64 encoding could be readily reversed to show the victim email address. Similarly, the victim email address itself is obfuscated to protect their privacy.



**Figure 2 – Sample Spearphishing Login Page And URL Path**

28. Thallium uses a variety of domain and subdomain themes to deceive victims into clicking or otherwise interacting with the domains. Some domains and subdomains have a webmail provider theme, such as “office356-us[.]org,” “outlook.mail[.]info,” “maingoogle[.]com,” or “inbox-yahoo[.]com,” while others mimic the victim’s organizations, such as “unite.un.graphwin[.]com,” “unite.office356-us[.]org,” or “naver.com-change[.]pw.” The bulk of Thallium’s domains however are generic but follow a pattern like “word-word[.]TLD,” such as “dialy-post[.]com,” “day-post[.]com,” or “app-wallet[.]com.” Some such domains used by Thallium are associated with servers used to control the operation of malicious software (“malware”) surreptitiously installed by Thallium on victim computers. For example,

such domains may send commands to the malware or receive technical responses or stolen data from the malware. The domains also have the benefit of being inconspicuous so as not to attract attention from network administrators when they are reviewing network traffic logs. All of these types of domains may be referred to as “command and control domains” and the associated computer infrastructure may be referred to as “command and control infrastructure.”

29. In addition, Thallium has developed a technique where a victim clicking on a malicious link in an email is first connected to the command and control infrastructure and is then re-directed to [http://go.microsoft\[.\]com/](http://go.microsoft[.]com/), a legitimate Microsoft domain. This technique deceives and confuses victims into thinking the link is not compromised because the domain is Microsoft’s and incorporates Microsoft’s trademarks and branded material. Even though the victim is ultimately redirected to a Microsoft domain, Thallium first registers the victim’s access to the command and control infrastructure to further carry out the malicious activity described in this declaration. For example, **Figure 3** below reflects that the malicious Thallium domain “seoulhobi[.]biz,” deceptively redirects the victim to a real Microsoft website containing Microsoft’s trademarks, in order to make a deceptive use of a legitimate Microsoft webpage, including the “Microsoft,” “Office,” “Windows,” “Surface,” “Xbox,” “HoloLens,” and “Azure” trademarks. The Thallium defendants carry out this technique in order to obfuscate their malicious activities. For example, researchers or other parties who are looking for malicious activities or accidentally browse to this domain may not understand that there is any malicious activity associated with it because it displays legitimate Microsoft content, which is actually displayed on a legitimate Microsoft website. Similarly, when the domain is being used for malicious purposes to target victims, the victim will be completely unaware of this fact because they are deceptively redirected to a legitimate Microsoft website that causes them to believe that the site is trustworthy, when in fact it is malicious and actively delivering malware.



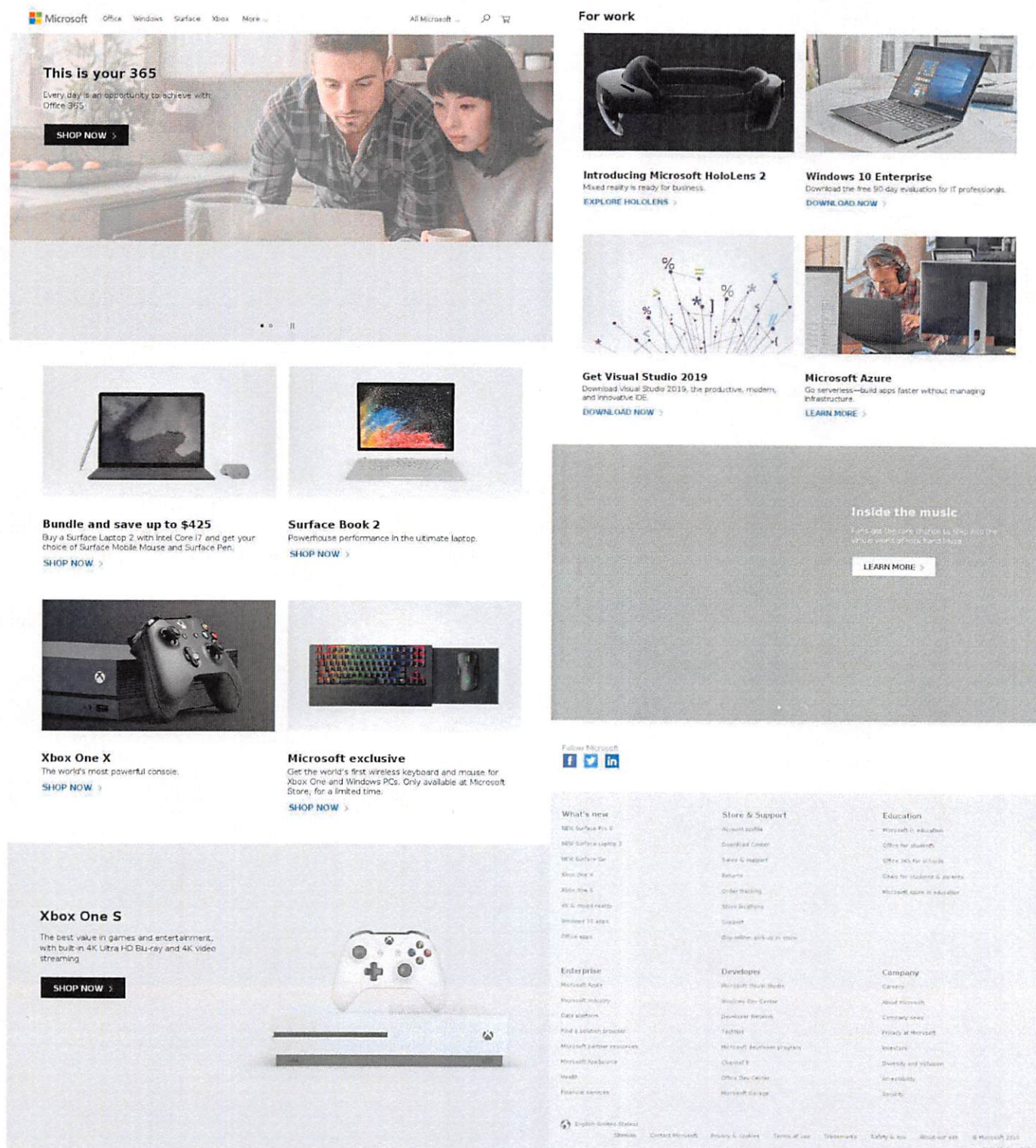


Figure 3 – Fraudulent Use Of Microsoft Website And Trademarks

30. Through research and investigation, Microsoft has determined that Thallium

currently uses the domains identified in **Appendix A** to this Complaint in its command and control infrastructure. The Thallium defendants sometimes disguise their command and control infrastructure by incorporating into the names of its command and control domains the names and trademarks of some well-known companies and organizations, including Microsoft, Google, Yahoo, and Naver (a South Korean online platform). As seen in **Appendix A** to this Complaint, Thallium has registered domains that contain Microsoft's brands and trademarks as disguises. Thallium's use of Microsoft brands and trademarks is meant to confuse Microsoft's customers into clicking on malicious links that they believe are associated and owned by Microsoft. As noted above, by tricking victims into clicking on the fraudulent links and providing their credentials, the Thallium defendants are then able to log into the victim's account. Additionally, the Thallium defendants can read sensitive and personal emails within the account, create new inbox rules including auto-forwarding, access the victim's contact list, send additional spearphishing emails to the victim's contacts, and hide traces of this malicious activity in the victim account by deleting emails. Customers expect Microsoft to provide safe and trustworthy products and services. There is a great risk that Microsoft's customers, both individuals and the enterprises they work for, may incorrectly attribute these problems to Microsoft's products and services, thereby diluting and tarnishing the value of these trademarks and brands.

31. In addition to targeting user's credentials, the Thallium defendants also utilize malware – the most common being indigenous implants named “BabyShark” and “KimJongRAT” – to compromise systems and steal data from victim systems. The Thallium defendants use misleading domains and Microsoft's trademarks to cause victims to click on the links that result in installation of this malware on the victims' computers. Once installed on a victim's computer, this malware exfiltrates information from the victim computer, maintains a persistent presence on the victim computer, and waits for further instructions from the Thallium

defendants.

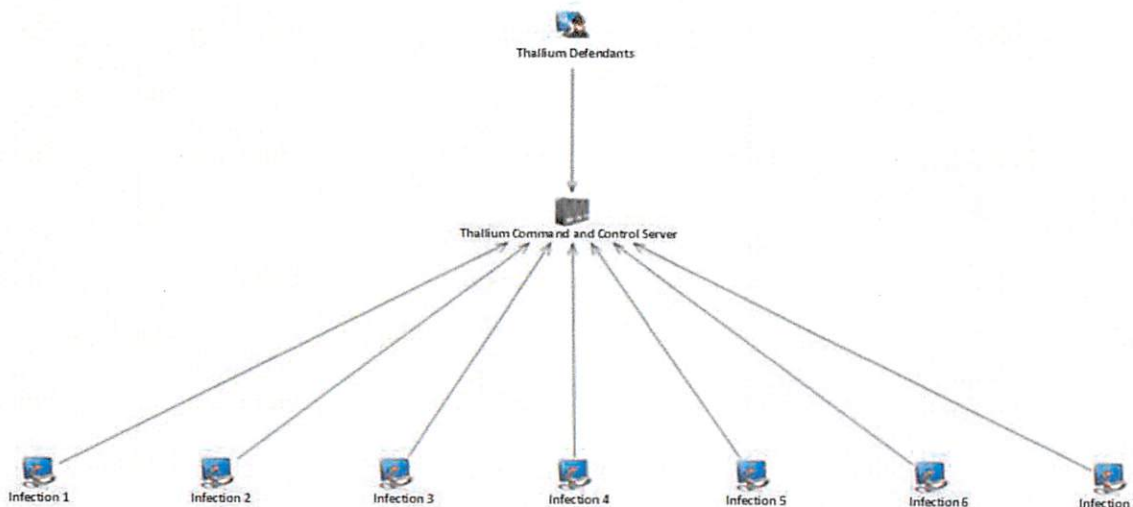
32. Samples of the KimJongRAT malware were observed dating back to 2010. The BabyShark malware is frequently sent to users as a malicious attachment to an email. The malware will drop a file with the file extension “.hta.” That file will then send a command that will beacon out to obtain an encoded script that is delivered back to the victim computer. The malware enables all future macros for Microsoft Word and Excel by adding the following registry keys taking away the user’s ability to disable macros:

HKCU\Software\Microsoft\Office\14.0\Excel\Security\VBAWarnings,value:1
HKCU\Software\Microsoft\Office\15.0\Excel\Security\VBAWarnings,value:1
HKCU\Software\Microsoft\Office\16.0\Excel\Security\VBAWarnings,value:1
HKCU\Software\Microsoft\Office\14.0\WORD\Security\VBAWarnings,value:1
HKCU\Software\Microsoft\Office\15.0\WORD\Security\VBAWarnings,value:1
HKCU\Software\Microsoft\Office\16.0\WORD\Security\VBAWarnings,value:1

33. From there, details and information from the victim computer are saved to victim’s computer in the Windows operating system file: %appdata%\Microsoft\ttmp.log. These details from the victim computer in the ttmp.log are then, ultimately, sent to one of the command and control servers of the Thallium defendants. From there, the Thallium defendants can send additional instructions and commands to the victim’s computer, and can exfiltrate additional stolen information from that computer. By specifically targeting Microsoft’s Windows operating system and utilizing registry and file paths containing Microsoft’s trademarks, in order to deceive users and carry out the fraudulent scheme, the Thallium defendants infringe Microsoft’s trademarks and deceptively use those trademarks in the context of Microsoft’s Windows operating system.

34. **Figure 4** reflects the relationship between the Thallium command and control

servers, associated with particular command and control domains, which interact with and receive information from computers infected with the BabyShark and KimJongRAT malware:



**Figure 4 – Thallium Command and Control Servers**

### **FIRST CLAIM FOR RELIEF**

#### **Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030**

35. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 34 above.

36. Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and knowingly caused the transmission of a program, information, code and commands, resulting in damage to the protected computers, the software residing thereon, and Microsoft.

37. Defendants' conduct involved interstate and/or foreign communications.



38. Defendants' conduct has caused a loss to Microsoft during a one-year period aggregating at least \$5,000.

39. Microsoft seeks injunctive relief and compensatory and punitive damages under 18 U.S.C. §1030(g) in an amount to be proven at trial.

40. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

### **SECOND CLAIM FOR RELIEF**

#### **Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701**

41. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 40 above.

42. Microsoft's Windows operating system software, and Microsoft's customers' computers running such software, and Microsoft's cloud-based services, such as Hotmail, Outlook and Office 365, are facilities through which electronic communication service is provided to Microsoft's users and customers.

43. Defendants knowingly and intentionally accessed the Windows operating system and Microsoft's Hotmail, Outlook and Office 365 software, services and computers upon which this software and services run without authorization or in excess of any authorization granted by Microsoft or any other party.

44. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and electronic communications transmitted via Microsoft's Windows operating system software and Microsoft's Hotmail, Outlook and Office 365 services and the computers running such software and services.

45. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

46. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

### **THIRD CLAIM FOR RELIEF**

#### **Trademark Infringement Under the Lanham Act – 15 U.S.C. § 1114 *et seq.***

47. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 46 above.

48. Defendants have used Microsoft's trademarks in interstate commerce, including Microsoft's federally registered trademarks for the word marks Microsoft®, Windows®, Hotmail®, Outlook®, MSN®, and Office365®, among other trademarks.

49. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act.

50. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

51. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which they have no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

52. Defendants' wrongful and unauthorized use of Microsoft's trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq.*

### **FOURTH CLAIM FOR RELIEF**

#### **False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a)**

53. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 52 above.

54. Microsoft's trademarks are distinctive marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

55. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants create false designations of origin as to tainted Microsoft products that are likely to cause confusion, mistake, or deception.

56. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Lanham Act, 15 U.S.C. § 1125(a).

57. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

58. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

#### **FIFTH CLAIM FOR RELIEF**

##### **Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c)**

59. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 58 above.

60. Microsoft's trademarks are famous marks that are associated with Microsoft and exclusively identify its businesses, products, and services.

61. Defendants make unauthorized use of Microsoft's trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Microsoft's trademarks.

62. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

63. As a direct result of Defendants' actions, Microsoft has suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

**SIXTH CLAIM FOR RELIEF**

**Cybersquatting under the Anti-Cybersquatting Consumer Protection Act – 15 U.S.C. §  
1125(d)**

64. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 63 above.

65. Microsoft's trademarks were distinctive at the time Defendants registered the command and control domains and remain distinctive today.

66. Microsoft's trademarks were famous at the time Defendants registered the command and control domains and remain famous today.

67. The command and control domains are confusingly similar to or dilutive of Microsoft's trademarks.

68. Defendants have registered, trafficked in, and/or used the command and control domains with bad faith with intent to profit from Microsoft's trademarks. As a result of their wrongful conduct, Defendants are liable to Microsoft for violation of the Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d).

**SEVENTH CLAIM FOR RELIEF**

**Common Law Trespass to Chattels**

69. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 68 above.

70. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

71. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to trespass on the computers and computer networks of Microsoft and its customers.

72. Defendants' actions in operating Thallium result in unauthorized access to Microsoft's Windows operating system and Internet Explorer software and the computers on which such programs run, and result in unauthorized intrusion into those computers and theft of information, account credentials, and funds.

73. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

74. Defendants' actions have caused injury to Microsoft and have interfered with the possessory interests of Microsoft over its software.

75. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

76. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

#### **EIGHTH CLAIM FOR RELIEF**

##### **Unjust Enrichment**

77. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 76 above.

78. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft in violation of the common law. Defendants used, without authorization or license, software belonging to Microsoft to facilitate unlawful conduct inuring to the benefit of Defendants.

79. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's intellectual property.

80. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of Microsoft's intellectual property.

81. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

82. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten profits.

83. As a direct result of Defendants' actions, Microsoft suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

#### **NINTH CLAIM FOR RELIEF**

##### **Conversion**

84. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 83 above.

85. Microsoft owns all right, title, and interest in its Windows software and the Hotmail, Outlook and Office365 software and services. Microsoft licenses its software to end-users. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Windows software and its Hotmail, Outlook and Office365 software and services.

86. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to remove, halt, or otherwise disable computer data, computer

programs, and computer software from a computer or computer network.

87. Defendants have, without authority, used a computer and/or computer network, without authority, with the intent to cause a computer to malfunction.

88. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including without limitation the return of Defendants' ill-gotten profits.

89. As a direct result of Defendants' actions, Microsoft suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

#### **TENTH CLAIM FOR RELIEF**

##### **Intentional Interference with Contractual Relationships**

90. Microsoft incorporates by reference each and every allegation set forth in paragraphs 1 through 89 above.

91. Microsoft has valid and subsisting contractual relationships with licensees of its Windows, Hotmail, Outlook and Office 365 products. Microsoft's contracts confer economic benefit on Microsoft.

92. Defendants' conduct interferes with Microsoft's contractual relationships by impairing, and in some instances destroying, the products and services Microsoft provides to its customers. On information and belief, Defendants know that their conduct is likely to interfere with Microsoft's contracts and to deprive Microsoft of the attendant economic benefits.

93. On information and belief, Microsoft has lost licensees due to Defendants' conduct.

94. Defendants' conduct has caused Microsoft economic harm. Microsoft seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial.

95. As a direct result of Defendants' actions, Microsoft has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs prays that the Court:

1. Enter judgment in favor of Microsoft and against the Defendants.
2. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice and oppression.
3. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein.
4. Enter a preliminary and permanent injunction giving Microsoft control over the domains used by Defendants to cause injury and enjoining Defendants from using such instrumentalities.
5. Enter judgment awarding Plaintiffs actual damages from Defendants adequate to compensate Plaintiffs for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial.
6. Enter judgment disgorging Defendants' profits.
7. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial.



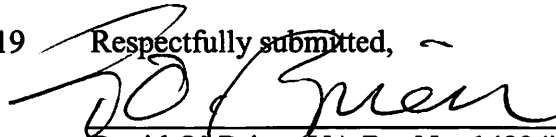
8. Enter judgment awarding attorneys' fees and costs, and
9. Order such other relief that the Court deems just and reasonable.

**DEMAND FOR JURY TRIAL**

Microsoft respectfully requests a trial by jury on all issues so triable in accordance with  
Fed. R. Civ. P. 38.

Dated: December 18, 2019

Respectfully submitted,



David O'Brien (VA Bar No. 14924)

CROWELL & MORING LLP  
1001 Pennsylvania Avenue NW  
Washington DC 20004-2595  
Telephone: (202) 624-2500  
Fax: (202) 628-5116  
dobrien@crowell.com

Gabriel M. Ramsey (*pro hac vice*)  
Kayvan Ghaffari (*pro hac vice*)  
CROWELL & MORING LLP  
3 Embarcadero Center, 26th Floor  
San Francisco, CA 94111  
Telephone: (415) 986-2800  
Fax: (415) 986-2827  
gramsey@crowell.com  
kghaffari@crowell.com

Richard Domingues Boscovich (*pro hac vice*)  
MICROSOFT CORPORATION  
One Microsoft Way  
Redmond, WA 98052-6399  
Telephone: (425) 704-0867  
Fax: (425) 936-7329  
rbosco@microsoft.com

*Attorneys for Plaintiff Microsoft Corp.*